On QMA Protocols with Two Short Quantum Proofs (New Trends in Algorithms and Theory of Computation)

AUTHOR(S):

Le Gall, Francois; Nakagawa, Shota; Nishimura, Harumichi

数理解析研究所講究録
第1799巻 2012年 73-80

2011年度冬のLAシンポジウム [16]

On QMA Protocols with Two Short Quantum Proofs

François Le Gall* Shota Nakagawa† Harumichi Nishimura‡

Abstract. This paper gives a QMA (Quantum Merlin-Arthur) protocol for 3-SAT with two logarithmic-size quantum proofs (that are not entangled with each other) such that the gap between the completeness and the soundness is $\Omega(\frac{1}{n\mathrm{polylog}(n)})$. This improves the best completeness/soundness gaps known for NP-complete problems in this setting.

1 Introduction

The quantum complexity class **QMA** [9, 10, 18] is a quantum analogue of the complexity class **NP** (or of the class **MA**). That is, a decision problem is in **QMA** if there is a polynomial-time quantum algorithm V (called the *verifier*) that satisfies the following two properties: (completeness) V accepts any yes-instance with probability $\geq a$ by the help of a quantum state (called a *quantum proof*); (soundness) V accepts any no-instance with probability $\leq b$ $(< a)$ whatever quantum state is provided. Bounding from below the gap between completeness and soundness $a-b$ by a positive constant (or an inverse polynomial) is enough since efficient gap amplification is possible (see, e.g., [9]).

Several variants of **QMA**, whose classical counterparts are uninteresting, have been introduced in the literature. One variant is the case where the verifier receives multiple quantum proofs that are unentangled with one another, which was first considered by Kobayashi, Matsumoto, and Yamakami [11]. Unexpectedly from the classical case, multiple quantum proofs may be more helpful than one proof since the verifier can use the fact that these proofs are not entangled to improve the soundness. In fact, Liu, Christandl, and Verstraete [12] found a problem that can be verified in quantum polynomial time using multiple quantum proofs but is not known to be in **QMA**. Recently, Harrow and Montanaro [8] showed that two quantum proofs are enough to obtain the full power of multiple quantum proofs by proving that efficient gap amplification is possible (note that it was shown before that the number of quantum proofs can be reduced to two if and only if efficient gap amplification is possible [1, 11]). Another variant is the case where the verifier receives only a logarithmic-size quantum proof. Marriott and Watrous [14] showed that, similarly to the classical case, a logarithmic-size quantum proof is useless, that is, such a variant of **QMA** collapses to **BQP**, by proving that efficient gap amplification, where the proof must be kept to be logarithmic-size, is possible.

A combination of the above two variants (multiple quantum proofs with logarithmic length) was first studied by Blier and Tapp [3]. They showed that an NP-complete problem such as the 3-coloring problem can be verified in quantum polynomial time only using two quantum proofs with logarithmic length, while the gap between com-

*Graduate School of Information Science and Technology, The University of Tokyo. E-mail: legall@is.s.u-tokyo.ac.jp
†School of Science, Osaka Prefecture University. E-mail: nakagawa.d94q@gmail.com
‡School of Science, Osaka Prefecture University. E-mail: hnishimura@mi.s.osakafu-u.ac.jp

pleteness and soundness is an inverse polynomial (note that it is unknown whether efficient gap amplification is possible). Moreover, Aaronson et al. [1] showed that 3-SAT can be efficiently verified with a constant completeness/soundness gap using $O(\sqrt{n}\text{polylog}(n))$ quantum proofs, each proof being of logarithmic length. These results thus give new evidences that multiple quantum proofs may be helpful.

This paper focuses on how much the completeness/soundness gap can be improved in QMA protocols using two quantum proofs with logarithmic length for NP-complete problems. The gap obtained by Blier and Tapp was $\Omega(\frac{1}{n^6})$. After that, Beigi [2] improved the gap to $\Omega(\frac{1}{n^{3+\epsilon}})$ for 3-SAT, where $\epsilon > 0$ is any constant. In the present work we further improve the gap to $\Omega(\frac{1}{n\text{polylog}(n)})$ for 3-SAT.

Independently of us, Chiesa and Forbes [6] also improved the completeness/soundness gap of QMA protocols with two logarithmic-size quantum proofs. They showed that the gap of the Blier-Tapp protocol can be improved to $\Omega(\frac{1}{n^2})$ by tightening the analysis. (In fact, two of the authors obtained the same conclusion before the present work [16].) The reason why our gap is better is simple: we combine the Blier-Tapp protocol with Dinur's PCP reduction [7]. However, we then need a complicated case-study analysis different from the one of [3], while the analysis in [6, 16] basically follows [3].

2 Preliminaries

In this section, we present technical tools that are used to obtain our result. All of the tools have already been used previously [3, 5] for studying QMA protocols using multiple quantum proofs with logarithmic length but we state them for self-containedness.

The first group of our tools, which was used in [3], consists of the distance between (pure) quantum states, the distance between probability distributions, the relation between their distances, and a basic fact on the swap test [4].

Definition 1 *(Quantum distance)* $D(|\Psi\rangle, |\Phi\rangle) := \sqrt{1 - |\langle\Psi|\Phi\rangle|^2}$.

Definition 2 *(Classical distance) Let* $P = \{p_1, \ldots, p_k\}$ *and* $Q = \{q_1, \ldots, q_k\}$ *be two probability distributions. Then,* $D(P, Q) := \frac{1}{2}\sum_{i=1}^{k} |p_i - q_i|$.

Theorem 1 *(Relationship between the quantum and classical notions of distance [17]) Let* M *be a von Neumann measurement. Let* P *and* Q *be the distributions of outcomes when performing* M *on* $|\Psi\rangle$ *and* $|\Phi\rangle$*, respectively. Then,* $D(|\Psi\rangle, |\Phi\rangle) \geq D(P, Q)$.

Theorem 2 *(Swap test [4]) When performing the swap test on* $|\Psi\rangle$ *and* $|\Phi\rangle$*, the probability that the test outputs NO (which means the two states are not equal) is* $\frac{1}{2} - \frac{|\langle\Psi|\Phi\rangle|^2}{2}$.

The second group of our tools is from Dinur's PCP theorem [7], which was used in [5]. We present necessary terminologies and Dinur's PCP reduction, following the description given in [5].

Definition 3 *(Constraint graph) A* constraint graph $G = (V(G), E(G))$ *is an undirected graph (possibly with self-loops) along with a set* Σ *of "colors" and mappings* $R_e : \Sigma \times \Sigma \to \{0, 1\}$ *for each edge* $e = (v, u) \in E(G)$ *(called the* constraint *to* e*). A mapping* $\tau : V(G) \to \Sigma$ *(called a* coloring*) satisfies the constraint* R_e *if* $R_e(\tau(v), \tau(u)) = 1$ *for an edge* $e = (v, u) \in E(G)$*. The graph* G *is said to be* satisfiable *if there is a coloring* τ *that satisfies all constraints, while* G *is said to be* $(1 - \eta)$-unsatisfiable *if for all colorings* τ*, the fraction of constraints satisfied by* τ *is at most* $1 - \eta$.

Theorem 3 *[7] There exists a mapping T from 3-SAT instances to constraint graphs with the following properties.*

- *(Completeness) If ϕ is a satisfiable formula, $T(\phi)$ is a satisfiable constraint graph.*
- *(Soundness) There exists an absolute constant $\eta > 0$ such that if ϕ is unsatisfiable formula, $T(\phi)$ is $(1-\eta)$-unsatisfiable.*
- *(Size-Efficiency) If ϕ has m clauses, then $|V(T(\phi))| = O(m\text{polylog}(m))$ and $|E(T(\phi))| = O(m\text{polylog}(m))$. (The value $|V(T(\phi))|$ will usually be denoted in this paper by n.)*
- *(Alphabet Size) $|\Sigma| = K > 1$ is a constant independent of m.*
- *(Regularity) $T(\phi)$ is a d-regular graph (with self-loops), where d is a constant independent of m.*

3 Our Result

We first recall the formal definition of the quantum complexity class $\mathbf{QMA}_{\log}(2, a, b)$, which is the set of languages that can be verified in quantum polynomial time using two logarithmic-size quantum proofs. In what follow, let $\mathcal{H}_\ell = \text{span}\{|0\rangle, |1\rangle, \ldots, |\ell-1\rangle\}$ for any value $\ell \geq 1$.

Definition 4 *A language L is in $\mathbf{QMA}_{\log}(2, a, b)$ if there exists a polynomial-time quantum algorithm V (verifier) and a constant c such that for any n and any instance x of length n the following two conditions hold:*

(Completeness) *If $x \in L$, there exists a state $|\Psi\rangle \otimes |\Phi\rangle \in \left(\mathcal{H}_2^{c\log(n)}\right)^{\otimes 2}$ (two quantum proofs) such that V accepts with probability at least a.*

(Soundness) *If $x \notin L$, then for all states $|\Psi\rangle \otimes |\Phi\rangle \in \left(\mathcal{H}_2^{c\log(n)}\right)^{\otimes 2}$, the probability that V accepts is at most b.*

Our result is the following theorem where a 3-SAT instance has n clauses.

Theorem 4
3-SAT is in $\mathbf{QMA}_{\log}\left(2, 1, 1 - \Omega(\frac{1}{n\text{polylog}(n)})\right)$.

There are a few remarks about this theorem. First, our result keeps perfect completeness similarly to the Blier-Tapp's result [3] (and the recent improvement of the gap to $\Omega(\frac{1}{n^2})$ [6, 16]). Second, our protocol is applicable to other NP-complete problems for which Theorem 3 holds (e.g., the 3-coloring problem).

To prove Theorem 4, in view of Theorem 3 it suffices to show the following theorem.

Theorem 5 *There is a QMA protocol with two logarithmic-size quantum proofs such that for any constraint graph $G = (V(G), E(G))$ obtained from 3-SAT instances by the mapping of Theorem 3 (where $n = |V(G)|$):*

(Completeness) *If G is satisfiable, then there exist two logarithmic-size quantum proofs $|\Psi\rangle$ and $|\Phi\rangle$ such the verifier accepts with probability* 1.

(Soundness) *If G is $(1-\eta)$-unsatisfiable, the verifier accepts with probability at most $1 - \Omega(\frac{1}{n})$ for any two logarithmic-size quantum proofs $|\Psi\rangle$ and $|\Phi\rangle$.*

In the next section, we prove Theorem 5. The verifier's protocol is described in Section 4.1. Section 4.2 discusses its completeness, and Section 4.3 discusses its soundness, which is our main technical part.

4 Proof of Theorem 5

Recall that n stands for the number of vertices of a given constraint graph $G = (V(G), E(G))$, and K is the alphabet size. We denote the quantum Fourier transform on $\mathcal{H}_k$ by F_k.

4.1 Protocol

As mentioned before, our protocol is obtained by incorporating Dinur's PCP reduction into the Blier-Tapp protocol. Similarly to the Blier-Tapp protocol, the protocol of the verifier consists of three tests: the equality test, the consistency test, and the uniformity test. The verifier expects to receive, as the two proofs, the same uniform superpositions of all vertices and their coloring $(i, \tau(i))$,

$$\frac{1}{\sqrt{n}} \sum_i |i\rangle|\tau(i)\rangle,$$

which we call a *proper* state (whose name follows similar concepts in [1, 2]). Suppose that the two proofs are proper and the same. Then the consistency test will check if the coloring is really valid: by measuring the two proofs in the computational basis, we obtain two vertices and their colors (i, j) and (i', j'), and then we can check whether edge (i, i') satisfies the constraint (or whether $j = j'$ if $i = i'$). For any no-instance, we can find the inconsistency with a better probability than previous works [3, 6, 16] because our protocol uses Dinur's PCP reduction, which guarantees the existence of many edges that do not satisfy the constraint. The equality test can be used for checking whether the two proofs are really the same via the swap test. Finally, whether the proofs are proper or not can be checked by the combination of the consistency test and the uniformity test.

The protocol of the verifier is now formally given as follows.

Verifier's protocol for instance G

Suppose that $|\Psi\rangle$ and $|\Phi\rangle$ on $\mathcal{H}_n \otimes \mathcal{H}_K$ are given to the verifier as the two quantum proofs. The verifier then performs, with equal probability, one of the following three tests on $\mathcal{H}_n \otimes \mathcal{H}_K$. If he does not reject, then he accepts. We call the first part of $\mathcal{H}_n \otimes \mathcal{H}_K$ the vertex register and the second part of $\mathcal{H}_n \otimes \mathcal{H}_K$ the color register.

(Equality test). Perform the swap test [4] on $|\Psi\rangle$ and $|\Phi\rangle$, and reject if the test outputs NO.

(Consistency test). Measure the two states $|\Psi\rangle$ and $|\Phi\rangle$ in the computational basis, yielding the outcomes (i, j) and (i', j'), respectively. Then, do as follows:
a) If $i = i'$, verify that $j = j'$. Reject if $j \neq j'$.
b) If $i \neq i'$ and $(i, i') \in E(G)$, verify that $R_{(i,i')}(j, j') = 1$. Reject if $R_{(i,i')}(j, j') = 0$.

(Uniformity test). For both $|\Psi\rangle$ and $|\Phi\rangle$, do as follows: The Fourier transform F_K is applied on the color register, which is then measured in the computational basis. If the outcome is 0, the inverse Fourier transform $F_n^\dagger$ is applied on the vertex register, which is then measured in the computational basis. Reject if the second outcome is not 0.

4.2 Completeness

The following theorem shows that our protocol has perfect completeness.

Proposition 1 *If G is satisfiable, then there exist two quantum proofs $|\Psi\rangle$ and $|\Phi\rangle$ such that the verifier accepts with probability 1.*

Proof. Take $|\Psi\rangle = |\Phi\rangle = \frac{1}{\sqrt{n}}\sum_i |i\rangle|\tau(i)\rangle$ where τ is a coloring that satisfies all constraints. Since $|\Psi\rangle = |\Phi\rangle$, the verifier accepts with probability 1 in the equality test. Because τ satisfies the constraint R_e for any edge $e \in E(G)$, the verifier accepts with probability 1 in the consistency test. Finally, we analyze the uniformity test. The Fourier transform F_K is performed on the color register, and

$$\begin{aligned}&(I \otimes F_K)\frac{1}{\sqrt{n}}\sum_i |i\rangle|\tau(i)\rangle \\ =&\frac{1}{\sqrt{n}}\sum_i |i\rangle \frac{1}{\sqrt{K}}\sum_k \exp\left(\frac{2\pi\sqrt{-1}\tau(i)k}{K}\right)|k\rangle.\end{aligned}$$

So, if the outcome of the measurement of the color register is 0, the state of the vertex register is $\frac{1}{\sqrt{n}}\sum_i |i\rangle = F_n|0\rangle$. Therefore, the verifier accepts with probability 1 in the uniformity test. □

4.3 Soundness

What remains to show is the soundness of our protocol.

Proposition 2 *If G is $(1-\eta)$-unsatisfiable, the verifier rejects with probability at least $\Omega\left(\frac{1}{n}\right)$ for any two quantum proofs $|\Psi\rangle$ and $|\Phi\rangle$.*

In order to prove Proposition 2, we first describe general forms for the two quantum proofs. Because the two proofs are not entangled, they can be written separately as

$$\begin{aligned}|\Psi\rangle &= \sum_{i=0}^{n-1}\alpha_i|i\rangle\sum_{j=0}^{K-1}\beta_{i,j}|j\rangle, \\ |\Phi\rangle &= \sum_{i=0}^{n-1}\alpha'_i|i\rangle\sum_{j=0}^{K-1}\beta'_{i,j}|j\rangle, \end{aligned} \quad (1)$$

where $\sum_i |\alpha_i|^2 = 1$ and $\sum_j |\beta_{i,j}|^2 = 1$ for any i, and likewise for $|\Phi\rangle$. Next we give several lemmas. The first lemma guarantees that for every vertex i there is at least one relatively large $|\beta_{i,j}|$ (which means that j will be measured in the color register with a relatively high probability).

Lemma 1 *For every i, there exists at least one j such that $|\beta_{i,j}|^2 \geq \frac{1}{K}$. (Likewise for $\beta'_{i,j}$.)*

Proof. By contradiction. Suppose that $|\beta_{i,j}|^2 < \frac{1}{K}$ for every j. Then,

$$\sum_j |\beta_{i,j}|^2 < \frac{1}{K} \times K = 1.$$

This contradicts the condition $\sum_j |\beta_{i,j}|^2 = 1$. □

By definition we have $\sum_j |\beta_{i,j}|^2 = 1$. The second lemma shows that if $\left|\sum_j \beta_{i,j}\right|^2$ is small, then at least two different $|\beta_{i,j}|$ must be relatively large.

Lemma 2 *For every i, if $\left|\sum_j \beta_{i,j}\right|^2 < \frac{1}{100K}$, then there are at least two j's such that $|\beta_{i,j}|^2 \geq \frac{1}{K^4}$.*

Proof. By Lemma 1, we know that there exists an index j_0 such that $|\beta_{i,j_0}|^2 \geq \frac{1}{K} \geq \frac{1}{K^4}$. We work by contradiction and suppose that $|\beta_{i,j}|^2 \leq \frac{1}{K^4}$ for all the indexes $j \neq j_0$. Note that this implies that

$$\begin{aligned}\left|\sum_{j\neq j_0}\beta_{i,j}\right| &\leq \sum_{j\neq j_0}|\beta_{i,j}| \\ &\leq (K-1)\times\frac{1}{K^2} \\ &\leq \frac{1}{K}.\end{aligned}$$

Using the fact that the inequality $|a-b| \geq ||a|-|b||$ holds for any complex numbers a and b, we obtain:

$$\begin{aligned}\left|\sum_j \beta_{i,j}\right|^2 &= \left|\beta_{i,j_0} + \sum_{j\neq j_0}\beta_{i,j}\right|^2 \\ &\geq \left(|\beta_{i,j_0}| - \left|\sum_{j\neq j_0}\beta_{i,j}\right|\right)^2.\end{aligned}$$

Since $|\beta_{i,j_0}| - \left|\sum_{j \neq j_0} \beta_{i,j}\right| \geq \frac{1}{\sqrt{K}} - \frac{1}{K} \geq 0$ and $K > 1$, we conclude that

$$\left|\sum_j \beta_{i,j}\right|^2 \geq \frac{\left(1 - \frac{1}{\sqrt{K}}\right)^2}{K} \geq \frac{1}{100K},$$

which contradicts the assumption of the lemma. □

The following lemma follows trivially from Lemma 1, but we prefer to state it explicitly for later reference.

Lemma 3 *For every i, there exists at least one j such that $K|\beta_{i,j}|^2 \geq |\beta'_{i,j}|^2$ and $|\beta_{i,j}|^2 \geq \frac{1}{K}$. (For later reference, we denote such j by $j[i]$.)*

Proof. By Lemma 1, there exists an index j such that $|\beta_{i,j}|^2 \geq \frac{1}{K}$. Moreover, for the same j, $K|\beta_{i,j}|^2 \geq |\beta'_{i,j}|^2$ (since $K|\beta_{i,j}|^2 \geq K \times \frac{1}{K} = 1 \geq |\beta'_{i,j}|^2$). □

Now we are ready to prove Proposition 2.

Proof of Proposition 2. We first introduce the following subsets of $\{0, 1, \ldots, n-1\}$ (the set of possible i's). This will be the key of our analysis.

$$A = \left\{ i \;\middle|\; |\alpha_i|^2 < \frac{1}{5000K^3n} \right\},$$

$$B = \left\{ i \;\middle|\; \left|\sum_j \beta_{i,j}\right|^2 < \frac{1}{100K} \right\},$$

$$A' = \left\{ i \;\middle|\; |\alpha'_i|^2 < \frac{1}{10000K^4n} \right\},$$

and

$$C = \left\{ i \in \overline{A} \cap \overline{A'} \;\middle|\; ArgMax_j |\beta_{i,j}|^2 \neq ArgMax_j |\beta'_{i,j}|^2 \right\},$$

where, for any i, $ArgMax_j |\beta_{i,j}|^2$ represents the j that maximizes $|\beta_{i,j}|^2$ (when multiple such j's exist, the smallest one is taken). Let us describe intuitively the roles of the sets A, A', B and C. The set A (resp. A') will be used to analyze what happens when the distribution of the $|\alpha_i|$'s (resp. the distribution of the $|\alpha'_i|$'s) is far from uniform. The set B will be used to analyze what happens when $|\Psi\rangle$ contains many vertices with more than one color (via Lemma 2). The set C will be used to analyze what happens when there are many vertices whose color differs in $|\Psi\rangle$ and in $|\Phi\rangle$.

Next we consider the four disjoint sets A, $\overline{A} \cap A'$, $\overline{A} \cap \overline{A'} \cap B$ and $\overline{A} \cap \overline{A'} \cap \overline{B}$, which partition the set $\{0, 1, \ldots, n-1\}$. We have $\sum_{i \in \overline{A}} |\alpha_i|^2 \geq 0.99$ since

$$\begin{aligned} \sum_{i \in \overline{A}} |\alpha_i|^2 &= 1 - \sum_{i \in A} |\alpha_i|^2 \\ &\geq 1 - \frac{1}{5000K^3n} \times n \\ &= 1 - \frac{1}{5000K^3} \\ &\geq 0.99. \end{aligned}$$

Thus at least one of the three sums $\sum_{i \in \overline{A} \cap A'} |\alpha_i|^2$, $\sum_{i \in \overline{A} \cap \overline{A'} \cap B} |\alpha_i|^2$ and $\sum_{i \in \overline{A} \cap \overline{A'} \cap \overline{B}} |\alpha_i|^2$ is larger than 0.3. Now we analyze the following six cases.

1. $\sum_{i \in \overline{A} \cap A'} |\alpha_i|^2 \geq 0.3$. : **case 1**
2. $\sum_{i \in \overline{A} \cap \overline{A'} \cap B} |\alpha_i|^2 \geq 0.3$. : **case 2**
3. $\sum_{i \in \overline{A} \cap \overline{A'} \cap \overline{B}} |\alpha_i|^2 \geq 0.3$.
   - 3.1. $|A| \geq 0.05\eta n$. : **case 3**
   - 3.2. $|A| < 0.05\eta n$.
     - 3.2.1. $|A'| \geq 0.15\eta n$. : **case 4**
     - 3.2.2. $|A'| < 0.15\eta n$.
       - 3.2.2.1. $|C| \geq 0.01\eta n$. : **case 5**
       - 3.2.2.2. $|C| < 0.01\eta n$. : **case 6**

These six cases cover the six possibilities that can happen for a no-instance. Intuitively, case 1 is when

the two proofs are much different; this is rejected with high probability by the equality test. Case 2 is when the two proofs are similar but there are many vertices i for which at least two different colors have large amplitude; this can be rejected with high probability by part a) of the consistency test. Case 3 is when the two proofs are similar and most vertices have a unique color but the distribution of the weights $|\alpha_i|^2$ in $|\Psi\rangle$ is far from uniform; this is rejected with high probability by the uniformity test. Case 4 is when the distribution of the weights $|\alpha_i|^2$ in $|\Psi\rangle$ is close to uniform but the distribution of the weights $|\alpha'_i|^2$ in $|\Phi\rangle$ is far from uniform; this is rejected with high probability by the equality test. Case 5 is when there are many vertices such that their color in $|\Psi\rangle$ is different from their color in $|\Phi\rangle$; this is rejected with high probability by part a) of the consistency test. Finally, case 6 is when the two proofs are close to proper states; this is rejected with high probability by part b) of the consistency test due to the soundness of the PCP reduction.

We can show that the rejecting probability is $\Omega(\frac{1}{n})$ in each of the six cases. See the detailed analysis in the full version of this paper [13]. □

5 Concluding Remarks

We have shown that there is a QMA protocol for 3-SAT with two quantum proofs of logarithmic length such that the gap between completeness and soundness is $\Omega(\frac{1}{n\mathrm{polylog}(n)})$, which improves the previous works [3, 2, 6, 16].

It seems to be difficult to improve our current gap as long as a protocol similar to the Blier-Tapp one is used. Moreover, it can be shown that all the tests of our protocol are necessary. For example, we cannot delete the equality test (that uses the swap test) since, without it, perfect cheating becomes possible (i.e., there are quantum proofs such that the verifier accepts a no-instance with probability 1). This is different from the case of [5] where it was shown that the swap test can be eliminated while still obtaining the same conclusion as in [1] (namely, that 3-SAT can be verified in quantum polynomial time using $O(\sqrt{n}\mathrm{polylog}(n))$ quantum proofs with logarithmic length).

Notes. If you want to read Japanese version of this paper, see the paper [15].

Acknowledgements

We are grateful to Richard Cleve, Kazuo Iwama, Hirotada Kobayashi, Shuichi Miyazaki, and Junichi Teruyama for helpful discussions.

References

[1] S. Aaronson, S. Beigi, A. Drucker, B. Fefferman and P. W. Shor. The power of unentanglement. *Theory of Computing* **5(1)** (2009) 1–42. arXiv:0804.0802.

[2] S. Beigi. NP vs $\mathrm{QMA}_{\log}(2)$. *Quantum Information & Computation* **10** (2010) 141–151. arXiv:0810.5109.

[3] H. Blier and A. Tapp. All languages in NP have very short quantum proofs. *Proc. 3rd ICQNM*, pp.34–37, 2009. arXiv:0709.0738.

[4] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Physical Review Letters* **87** (2001) 167902. arXiv:quant-ph/0102001.

[5] J. Chen and A. Drucker. Short multi-prover quantum proofs for SAT without entangled measurements. arXiv:1011.0716.

[6] A. Chiesa and M. Forbes. Improved soundness for QMA with multiple provers. arXiv: 1108.2098.

[7] I. Dinur. The PCP theorem by gap amplification. *Journal of the ACM* **54(3)** (2007) 12.

[8] A. W. Harrow and A. Montanaro. An efficient test for product states with applications to quantum Merlin-Arthur games. *Proc. 51th FOCS*, pp.633–642, 2010. arXiv:1001.0017.

[9] A. Y. Kitaev, A. H. Shen and M. N. Vyalyi. *Classical and Quantum Computation*, American Mathematical Society, 2002.

[10] E. Knill. Quantum randomness and nondeterminism. Technical Report LAUR-96-2186, Los Alamos National Laboratory, 1996. arXiv:quant-ph/9610012.

[11] H. Kobayashi, K. Matsumoto and T. Yamakami. Quantum Merlin-Arthur proof Systems: Are multiple Merlins more helpful to Arthur? *Chicago Journal of Theoretical Computer Science* (2009) 3. arXiv:quant-ph/0306051.

[12] Y.-K. Liu, M. Christandl and F. Verstraete. Quantum computational complexity of the N-representability problem: QMA complete. *Physical Review Letters* **98(11)** (2007) 110503. arXiv:quant-ph/0609125.

[13] F. Le Gall, S. Nakagawa, H. Nishimura. On QMA Protocols with Two Short Quantum Proofs. arXiv:1108.4306.

[14] C. Marriott and J. Watrous. Quantum Arthur-Merlin games. *Computational Complexity* **14(2)** (2005) 122–152. arXiv:cs/0506068.

[15] S. Nakagawa. *Studies on QMA Protocols with Short Quantum Proofs.* Master Thesis, Osaka Prefecture University, February, 2012.

[16] S. Nakagawa and H. Nishimura. On the soundness of the Blier-Tapp QMA protocol. *Proc. 23rd Quantum Information Technology Symposium (QIT23)*, pp.132–135, 2010 (in Japanese). Available at http://www.mi.s. osakafu-u.ac.jp/ hnishimura/~NN10.pdf.

[17] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, 2000.

[18] J. Watrous. Succinct quantum proofs for properties of finite groups. *Proc. 41st FOCS*, pp.537–546, 2000. arXiv:cs/0009002.